

N.E. Please delete the amendment to page 53, line 53.

IN THE SPECIFICATION

Please replace the paragraph beginning at page 2, line 3, with the following rewritten paragraph:

---

\*Spam can also be a serious security problem. For instance, the Melissa virus and

B2 ExploreZip.worm have been spread almost exclusively via email attachments. Such viruses are usually dangerous only if the user opens the attachment that contains the malicious code, but many users open such attachments.\*

---

Please replace the paragraph beginning at page 4, line 7, with the following rewritten paragraph:

B3 \*The sending host's Message Transfer Agent 1001 sends an email message to the receiving host 1002. At step 1010, the sending MTA opens a TCP connection to the receiving host's reserved SMTP port. This is shown as a dashed line with an italics description to differentiate it from the subsequent protocol messages. This typically involves making calls to the Domain Name System (DNS) to get the IP address of the destination host or the IP address for a Message Exchange (MX) host for the domain. For example, the domain escom.com has a single MX host that lists the IP address 192.135.140.3. Other networks, particularly large Internet Service Providers (ISPs), might have multiple MX records that define a prioritized list of IP addresses to be used to send email to that domain.\*

---

Please replace the paragraph beginning at page 20, line 8 with the following rewritten paragraph:

B4  
Configuration databases include Trusted DB 1093, which is used to identify trusted networks that are permitted to bypass further filtering; Whitelist DB 1094, which contains individual email addresses that are permitted to bypass further filtering; Blacklist DB 1095, which identifies IP addresses of remote hosts that will be blocked immediately after they connect to the proxy server; Relay DB 1096, which contains configuration data for the Active Relay filter, including addresses of untrusted hosts that are known not to be dialup clients; Dialup DB 1097, which identifies untrusted hosts that are known not to be dialup clients; Configuration DB 1098, which includes general data such as the IP address and port for the Mailhost 1105, permissible domain names for RCPT messages, etc; and System Log 1099, as typically provided by the UNIX syslog facility or Windows NT Event Log service. The preferred embodiment is for each database to be provided as a separate file. However, alternative embodiments may provide for merging some or all databases into a single configuration database, however preferably excluding the Log 1099.

Please replace the paragraph beginning at page 25, line 20, with the following rewritten paragraph:

B5  
Cm.t  
Figure 13 provides an overview of the present invention, with more detailed operation shown in Figs. 14-29. The figure shows the key steps used by the Active Filter Proxy 1401 to validate a single email message from a remote host 1400 and transfer the message to the protected MTA 1402. A separate SMTP connection 1418 is used for actively probing the remote host in order to perform Active Dialup 1420 detection and Active Relay 1450 detection. An

B5  
Cmtd. additional connection may be established to a different mailhost for Active User testing. The Active filter Proxy 1401 corresponds to proxy 1104 shown in Fig. 7.

---

Please replace the paragraph beginning at page 26, line 11, with the following rewritten paragraph:

---

B6  
With respect to Internet standards, the present invention may be implemented without any changes to SMTP or any other protocol. Rather, this method uses multiple SMTP connections, appropriately synchronized to permit the proxy server to characterize the remote host 1400. Thus, the SMTP connection 1403 is initiated by the remote host 1400, and involves transactions 1410, 1413, 1480, 1484, 1488, 1493, and 1495. The SMTP connection 1418 is initiated by the Active Filtering proxy 1401, and involves transactions beginning at step 1450. This session is used only to acquire protocol responses from the remote host 1400. It does not actually send an email message from the proxy server 1401 to the remote host 1400. In addition, the proxy server 1401 makes other connections to DNS name servers and, if the connection 1418 fails, may make an SMTP connection to the Mail Exchange (MX) host for the address given in step 1413.

---

Please replace the paragraph beginning at page 28, line 6, with the following rewritten paragraph:

---

B6  
Cmtd. If the remote host does not pass the Active Relay test, including addresses of untrusted hosts that are known not to be relays, then the proxy 1401 conducts Active User testing 1901. Here the proxy identifies a mailhost responsible for processing mail to the supposed sender of

B7  
Cm d.d.

the message and queries that mailhost as to whether it will accept mail to that address. These protocol interactions are similar to those used in the Active Relay method but are not shown on Figure 13 since they do not usually involve the remote host 1400. If the configured mailhost for that address will not accept a reply to the MAIL From address, then the sender's address (i.e., the message) is probably forged, so the proxy 1401 sends an error message and immediately closes the connection. Active User testing is more fully discussed in relation to Figure 19.

---

Please ~~replace~~ the paragraph beginning at page 30, line 11, with the following rewritten paragraph:

---

B8

In all cases, the proxy host 1401 is preferably a Mail Exchange (MX) host for the local domain and is configured to listen on the SMTP port (TCP 25) for connections from remote hosts 1400. In the preferred embodiment, the proxy is configured to start a separate instance of the Active Filtering process when it receives the TCP connection to port 25. Thus, the proxy process 1401 handles a single message and exits when it has either rejected the message or transferred the message to the MTA.

---

Please ~~replace~~ the paragraph beginning at page 33, line 1 with the following rewritten paragraph:

---

B9  
Cm .t

The use of linear files for the trusted database and the blacklist database might not be optimal for performance in all networks. Accordingly, trusted domain names (e.g., "remote.dom") might preferably be maintained in a hashed dbm file. Blacklisted IP addresses might preferably be maintained in bitmap, a hashed list, dbm file, or even in Content addressable

A9  
Cmld. Memory (CAM) for increased performance. If the bit is set, then the block of addresses is  
blacklisted, otherwise it is acceptable.

---

Please replace the paragraph beginning at page 35, line 6, with the following rewritten  
paragraph:

---

A10  
In the preferred embodiment, the whitelist file is a text file that contains addresses (one  
per line) that are periodically mined from sendmail log entries for outgoing ("to=") messages.  
These log entries are for mail sent by the local organization to destination addresses on other  
networks, so adding these destination addresses to the whitelist file will ensure that the proxy  
will permit incoming email from those persons that local users have sent mail to. However, the  
whitelist database may be implemented as hashed db files, or even could be disabled. If the  
address matches a whitelist entry, processing continues with step 1470. The differences between  
the trusted database 1093 and the whitelist database 1094 is that for trusted hosts, mail is  
permitted from any user on the remote host to any user on the local host. For whitelist entries,  
mail is permitted only from the named user on the remote host to any user on the local host. -

---

Please replace the paragraph beginning at page 38, line 1, with the following rewritten  
paragraph:

---

All  
Cm.T The preferred embodiment uses a flat ASCII filed structure for the dialup database. If  
the requirement for non-dialup entries grow significantly, other representations (hashed db files,  
or CAM) may be desirable for performance reasons. If the IP address matches any entry, then  
the proxy 1401 bypasses any further dialup testing, and proceeds to step 1901. Relay testing is

A11  
Cmcd

not conducted since the filter has already determined that the reverse connection cannot be established to the remoter host at step 1419. If it does not match any entry in the non-dialup list, then it proceeds with dialup testing in step 1422.--

---

Please ~~replace~~ the paragraph beginning at page 50, line 13, with the following paragraph:

---

A12

--At step 1462, the proxy 1401 attempts to find if the IP address of the remote host 1400 matches a non-relay entry in the Relay database 1096 (Fig. 7). This database lists blocks of addresses that the local organization must exchange email with, but which would fail the relay test. There might typically be between about 5-50 entries in this database, with each entry covering a block of addresses. These entries can be pre-defined by a site survey performed by each organization, preferably before installing the Active Filtering proxy server. For simplicity, the preferred embodiment of the Relay Database 1096 (as with other IP addresses listed in steps 1406 and 1413) expresses these addresses as a dotted-quad IP address, a forward slash "/", and a number of bits to be matched. Other embodiments may use other representations (hashed db files, or CAM) for performance reasons.--

---

Please ~~replace~~ the paragraph beginning at page 53, line 21, with the following rewritten paragraph:

---

A13  
Cm.T

--The active relay method permits automatic rejection of all email sent from a user at an open relay host or relayed by an open relay host. However, in some cases it is necessary to override this behavior, for business or other reasons. For example, with respect to the bigisp example given above, the administrator of the Active Filtering proxy can configure the proxy to

A13  
Cmld

permit email sent from smallhost.dom and relayed by bigisp.dom by any one of the following actions: (1) defining bigisp.dom as a trusted domain, (2) defining smallhost.dom as a trusted domain, (3) adding a whitelist entry for the specific address "user@smallhost.dom", (3) or adding a non-relay entry for bigisp.dom, even though it is an open relay.

---

Please replace the paragraph beginning at page 56, line 1, with the following rewritten paragraph:

---

A14

With respect to Figure 19, the Active Filtering proxy 1401 begins operation at step 1901 subsequent to either Active Dialup or Active Relay testing. In step 1902, the proxy identifies a mailhost 1900 responsible for receiving mail to the MAIL From address 1413. The proxy searches the Domain Name System (DNS) information for the MAIL From domain for records identifying Mail Exchange (MX) hosts for that domain. MX records include a host name and preference value, and by convention the lowest preference value identifies the MX host that should be tried first. In the preferred embodiment, the proxy uses resolver library routines such as the DNS BIND res\_init() and res\_query() functions to access the MX records, however, other methods may be used to access the name server. If no MX host is found, then the proxy uses the MAIL From address (that is, the host name to the right of the "@" character in the MAIL From address) as the mailhost.

---

Please replace the paragraph beginning at page 56, line 11, with the following rewritten paragraph:

---

The step 1903, the proxy attempts to connect to the mail server identified in step 1902.

A15 This follows the same mechanisms described in step 1418, except that the TCP connection is to the identified mailhost 1900 rather than to the remote host 1400. If the connection is successful in step 1904, the proxy waits at step 1906 for the system greeting 1905 from the mailhost.

Otherwise, if the connection is unsuccessful, the preferred embodiment of the proxy simply proceeds to step 1470 for message transfer to the MTA. In alternative embodiments, the proxy might successively check for lower-preference MX hosts if the highest preference host is not available.

---